

# Layered Virus Protection for the Operations & Administrative Messaging System

---

Roger H. Cortez  
Jet Propulsion Laboratory  
October 12, 2002



# Contents

---

- The Need for Virus Protection
- Operations & Administrative Messaging
- Why Layered Protection?
- Virus Protection at the Workstation
- Virus Protection at the Mail Server
- Virus Protection at the SMTP Gateway
- Summary



# The Need for Virus Protection

---

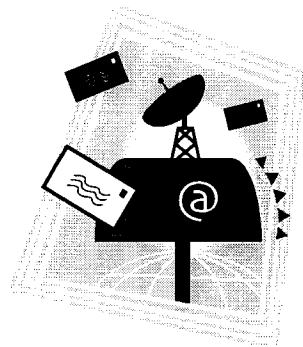
- Worms and viruses continue to increase in number and complexity
- Users are easily misled into opening infected attachments
- One infection can spread to hundreds of users within minutes
- Lost productivity for both the user and administrator
- Risk to operations

# Operations & Administrative Messaging (OAM)

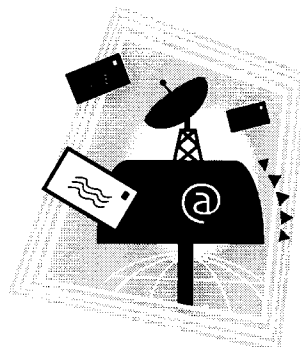
---

- Electronic mail system used by the Deep Space Network (DSN)
- Primary purpose is for sending/receiving messages that support DSN operations
- Built around Microsoft Exchange 5.5 and Windows NT 4.0
- Also used for administrative messaging

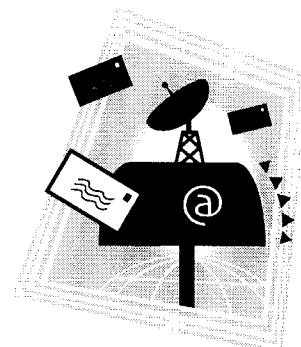
# OAM Server Locations



**Canberra DSCC**



**Goldstone DSCC**



**Madrid DSCC**



**Jet Propulsion Laboratory**



**JPL Foothill Facility**

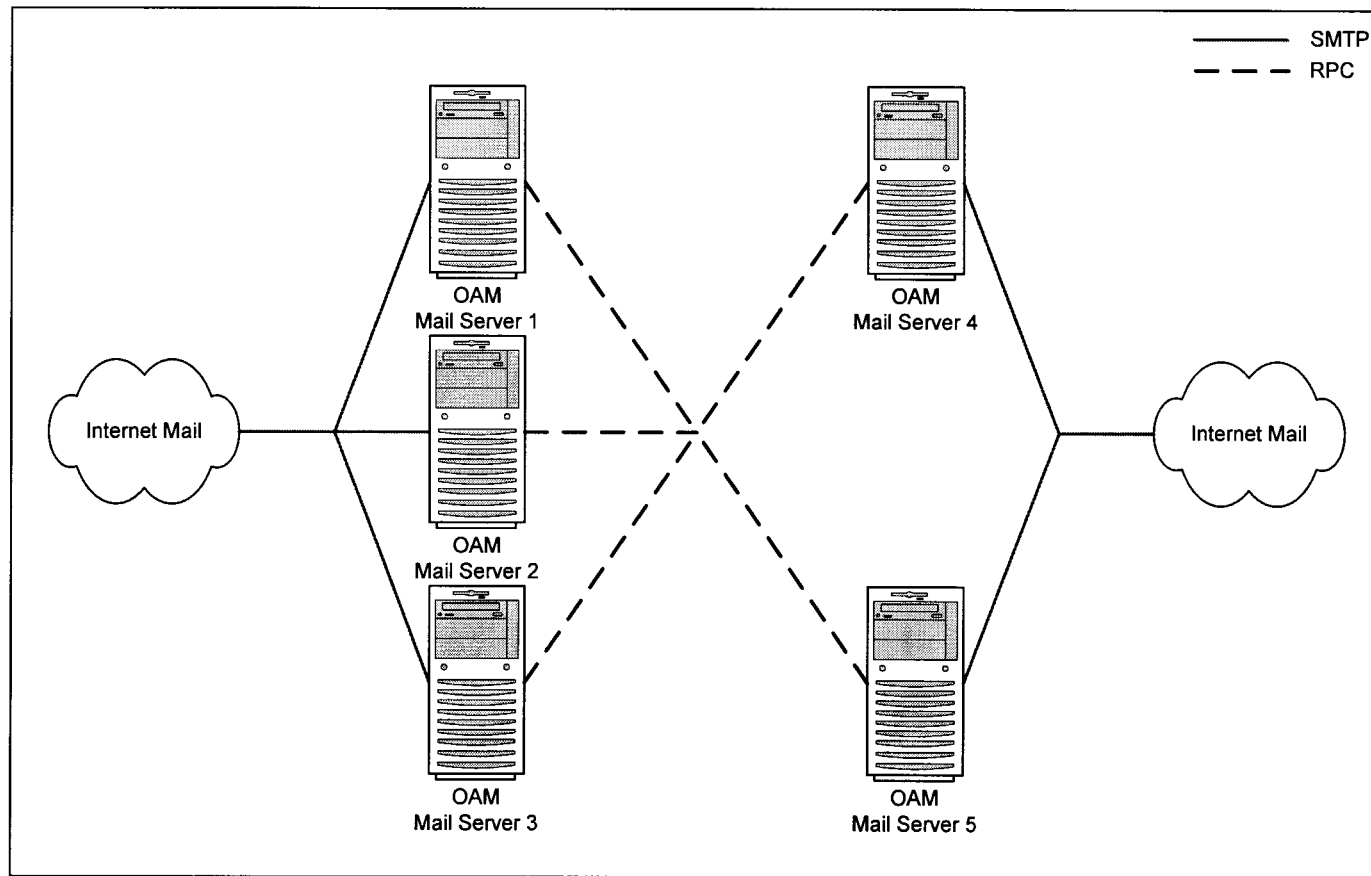
**DSCC – Deep Space Communication Complex**

10/12/2002

DRAFT

**JPL** 5

# Messaging Protocols



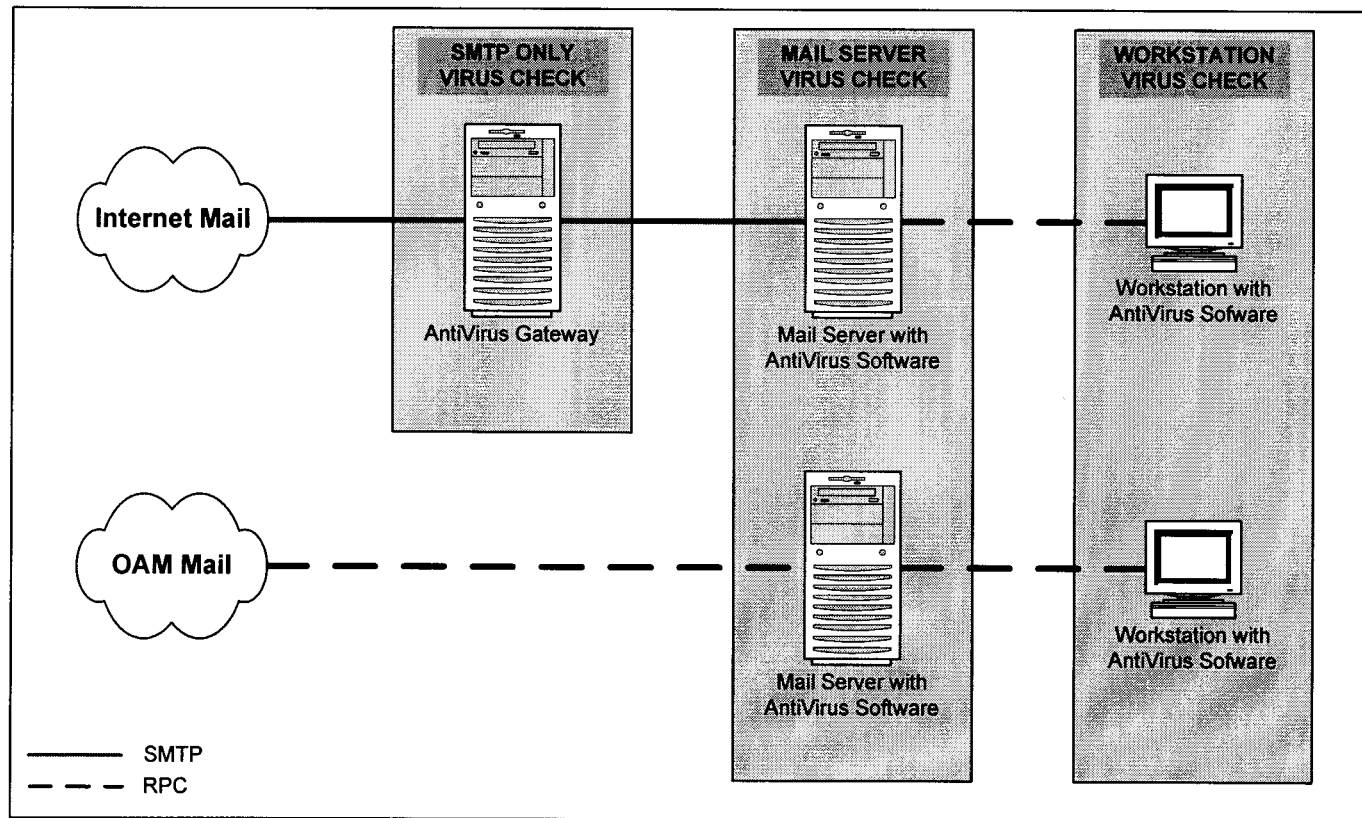


# Why Layered Protection?

---

- Single layer protection, typically at the workstation level, is no longer sufficient
  - Users disable or uninstall software
  - Virus definitions not always up to date
  - Does not protect against new or unknown viruses
- Multilayer protection minimizes risk by exposing potential viruses to different and multiple Anti-Virus software packages

# Layers of Protection





# AntiVirus at the Workstation

---

- Primary purpose is to protect the workstation from viruses that spread via alternate means
  - Network shares, file transfers, removable media
- Drawbacks
  - Users disable or uninstall software
  - Virus definitions not always up to date
  - May not protect against unknown viruses
- Recommendation – deploy managed clients



# AntiVirus at the Mail Server

---

- Industry standard AntiVirus software scans all messages for viruses
- Scans both Internet and OAM mail
- Drawbacks:
  - During virus outbreaks, new virus patterns must generally be manually updated
  - Does not protect against new or unknown viruses



# AntiVirus SMTP Gateway

---

- First layer of protection against messages originating from the Internet
- Virus definitions updated within minutes of their release
- Industry standard AntiVirus software scans all attachments
- Drawback:
  - Does not scan OAM mail



# AntiVirus SMTP Gateway

---

- But how do we protect against new, unknown viruses?
- Enforce additional rules at the SMTP Gateway
  - Quarantine all messages containing executable attachments
  - Quarantine all messages containing dangerous attachments (e.g. screen savers)
  - Scan messages for hostile code (e.g. Microsoft IFRAME vulnerability)



# Summary

---

- Single layer protection no longer sufficient
- Multilayer approach with virus protection at the gateway is essential
- Key is to protect against unknown or recently discovered viruses
  - Quarantine executable attachments
  - Quarantine dangerous attachments